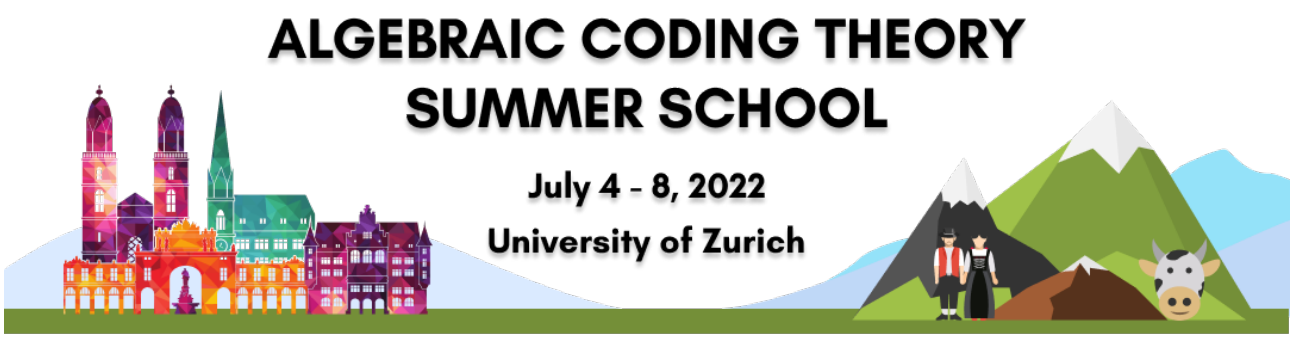

ACT22 Graduate Minisymposium

Friday, July 8th

09:20-11:00	*Giuseppe Cotardo*
	Paolo Santonastaso
	Benjamin Jany
	Avijit Panja
11:00-11:30	Coffee Break
11:30-13:10	*Felicitas Hörmann*
	Hedongliang Liu
	Rati Ludhani
	Lara Vicino
13:10-14:15	Lunch Break
14:15-15:30	*Charlene Weiß*
	Jonathan Mannaert
	Rumi Melih Pelen
15:30-16:00	Coffee Break
16:00-17:15	*Shikha Patel*
	José Manuel Muñoz
	Shikha Yadav

Funded by:

GRC GRANTS

UZH alumni

ZGSM uzh | eth | zurich

Abstracts

Session 1: 09:20 – 11:00

Giuseppe Cotardo, University College Dublin

Rank-Metric Lattices

In 1971, Dowling introduced a class of geometric lattices in connection with coding theory. The elements of these lattices are the $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ having a basis of vectors with Hamming weight bounded from above, ordered by inclusion. The theory of Dowling lattices and their extensions (called Higher-Weight Dowling Lattices, HWDL in short) have been brought forward by Bonin, Kung, and more recently by Ravagnani.

In this talk, we introduce the q-analogues of HWDLs, which we call rank-metric lattices (RML in short). Their elements are the $\mathbb{F}_{q^m}$-linear subspaces of $\mathbb{F}_{q^m}^n$ having a basis of vectors with rank weight bounded from above, ordered by inclusion. We determine which RMLs are supersolvable, computing their characteristic polynomials. We also investigate other structural properties of these lattices. In the second part of the talk, we establish a connection between RMLs and the problem of distinguishing between inequivalent rank-metric codes.

The new results in this talk are joint work with A. Ravagnani.

Paolo Santonastaso, Università degli Studi della Campania "Luigi Vanvitelli"

Optimal sum-rank metric codes

The equivalence classes of nondegenerate Hamming-metric codes are in one-to-one correspondence with equivalence classes of projective systems. Recently, Randrianarisoa and Sheekey showed that equivalence classes of nondegenerate rank-metric codes are in one-to-one correspondence with equivalence classes of q-systems. In this talk, we will explore a geometric point of view of sum-rank metric codes able to capture their structures, generalizing both projective systems and q-systems. Using this geometric connection, we will construct optimal codes in the sum-rank metric.

Benjamin Jany, University of Kentucky

The Projectivization Matroid of a q-Matroid.

q-Matroids, the q-analogue of matroids, were found useful in studying $\mathbb{F}_{q^m}$-linear rank metric codes. A q-matroid can be defined via a bounded, non-decreasing and submodular integer-valued rank function on the collection of subspaces of $\mathbb{F}_q^n$. Matroids are defined in an analogous way, where a rank function is defined on the collection of subsets of a finite set. It turns out an $\mathbb{F}_{q^m}$-linear rank metric code induces a q-matroid and many of the code's invariants can be determined from the associated q-matroid. In a similar way, a linear block code with the Hamming metric induces a matroid that captures the code's invariants. Given a q-matroid defined over $\mathbb{F}_q^n$, one can associate to it a matroid defined over the projective space $\mathbb{PF}_q^n$ called the projectivization matroid. The latter shares a similar flat structure than the q-matroid and therefore becomes a useful tool to study q-matroids. In this talk I will introduce the construction of the projectivization matroid and show that if the q-matroid arises form a rank metric code, then there exist a linear block code that induces the projectivization matroid. Using this connection, I will then show how one can derive a q-analogue of the critical theorem for q-matroids and $\mathbb{F}_{q^m}$-linear rank metric codes by studying the projectivization matroid.

Avijit Panja, Indian Institute of Technology Bombay

Some Matroids Related to Sum-Rank Metric Codes

We introduce the notion of sum-matroids and show its association with sum-rank metric codes. The sum-matroids generalize the notions of matroids and q-matroids. We define the generalized weights for sum-matroids and prove a Wei-type duality theorem which generalizes the analogous results for matroids and q-matroids. As a consequence, some results for sum-rank metric codes by Martínez-Peñas are generalized for sum-matroids.

This is a joint work with Rakhi Pratihar and Tovohery Randrianarisoa

---

Session 2: 11:30 – 13:10

Felicitas Hörmann, German Aerospace Center (DLR)

Error-Erasure Decoding in the Hamming, the Rank, and the Sum-Rank Metric

Channel models considering either errors or erasures in the Hamming metric arise naturally from communication systems and have been widely studied. Error-erasure decoders work on a channel that combines both error types and correct errors and erasures simultaneously. They proved useful for e.g. generalized minimum-distance (GMD) decoding of concatenated codes.

By now, the concept of erasures was also adapted to the rank and the sum-rank metric where the latter is a family of metrics containing the Hamming and the rank metric as special cases. In the sum-rank-metric setup, two notions of erasures are distinguished: row erasures, whose column space is known to the decoder as additional side information, and column erasures, for which the row space is known at the receiver. The talk will first discuss the intuition behind erasures in the three considered metrics and then focus on the problem of error-erasure decoding.

We finish with a short presentation of a current joint work that proposes the first error-erasure decoder for linearized Reed–Solomon codes in the sum-rank metric. The scheme can correct t_F full errors, t_R row erasures, and t_C column erasures as long as $2t_F + t_R + t_C \leq n - k$ holds for code length n and dimension k. It uses a Berlekamp–Massey-like approach and has quadratic complexity in the code length. Note that known error-erasure decoders for Reed–Solomon codes in the Hamming metric and for Gabidulin codes in the rank metric can be recovered as special cases.

Hedongliang Liu, Technical University of Munich

Quadratic Curve Lifted Reed-Solomon Codes

Lifted codes are a class of evaluation codes attracting more attention due to good locality and intermediate availability. In this work we introduce quadratic-curve-lifted Reed-Solomon (QC-LRS) codes, which is a class of bivariate evaluation codes and the codeword symbols whose coordinates are on a quadratic curve form a codeword of a Reed-Solomon code. We give upper and lower bounds on the dimension and show that the asymptotic rate of a QC-LRS code. Moreover, we provide analytical results on the minimum distance of this class of codes and compare QC-LRS codes with lifted Reed-Solomon codes by simulations in terms of the local recovery capability against erasures. For short lengths, QC-LRS codes have better performance in local recovery for erasures than LRS codes of the same dimension.

Rati Ludhani, Indian Institute of Technology Bombay

Minimum distance and the minimum weight codewords of Projective Reed-Muller Codes

Projective Reed-Muller codes, first introduced by Lachaud (1988), are an important variant of the well-known class of Reed-Muller codes. Define projective Reed-Muller codes on the field $\mathbb{F}_q$ of q elements and for the order d. We give an alternate proof for the minimum distance of projective Reed-Muller codes which was proved by Serre (1989) for the case $d \leq q+1$ and by Sørensen (1991) in the general case. Further, we give a characterization of minimum weight codewords of projective Reed-Muller codes.

This is a joint work with Sudhir R. Ghorpade.

Lara Vicino, Technical University of Denmark

Two-point AG codes from the Beelen-Montanucci maximal curve

Algebraic geometry codes (AG codes) are a family of error-correcting codes introduced by Goppa in the '80s and constructed using algebraic curves defined over a finite field. A general lower bound for the minimum distance of an AG code is given by the well-known Goppa bound, so that for a code $[n, k, d]$ whose underlying algebraic curve has genus g, the inequality $d \geq n - k + 1 - g$ holds, hence the minimum distance can be designed.

Let $\mathbb{F}_q$ be the finite field with q elements and X be an algebraic curve defined over $\mathbb{F}_q$ and of genus g. X is said to be maximal if it attains the Hasse-Weil bound, which means it has the largest number of rational points with respect to its genus. For this reason, maximal curves are suitable candidates for the construction of AG codes with good parameters.

In this talk, I will present some results on duals of two-point AG codes coming from the Beelen-Montanucci maximal curve. In particular, we used the order bound to compute a lower bound on the minimum distance that improves the Goppa bound. Our results rely on the study of a certain two-point Weierstrass semigroup on the Beelen-Montanucci curve, which we managed to determine completely.

Using these methods, we discovered AG codes with better parameters with respect to comparable two-point codes from the Garcia-Güneri-Stichtenoth (GGS) curve.

Joint work with Leonardo Landi.

Session 3: 14:15 – 15:30

Charlene Weiß, Paderborn University

The linear programming bounds for classical association schemes

Many interesting codes such as classical codes, rank-metric codes, and sub-space codes can be viewed as subsets of association schemes. The corresponding association schemes are called classical and consist of the Hamming scheme, the Johnson scheme, and several q-analogs of them. By using association schemes, Delsarte introduced a linear program that yields an upper bound for the size of codes. This linear program has been studied for many years in the case of the Hamming scheme and the Johnson scheme and it is still unknown what the exact solution of this program looks like. In this talk, by using a unified way, I will give the exact solution of the linear program for codes in the projective space, in the bipartite halves (Greeks and Latins) of the hyperbolic polar space, and in one of the Hermitian polar spaces, as well as for their affine counterparts: bilinear forms scheme, alternating forms scheme, and Hermitian forms scheme.

This is a joint work with Kai-Uwe Schmidt.

Jonathan Mannaert, Vrije Universiteit Brussel (VUB)

Some theoretical applications of association schemes

A Cameron-Liebler line class (CLLC) $\mathcal{L}$ in $\mathrm{PG}(n,q)$ or $\mathrm{AG}(n,q)$, for $n \geq 3$, is a set of lines for which its characteristic vector $\chi = \sum_{p \in \mathrm{PG}(n,q)} c_p \chi_p$. Here χ_p denotes the characteristic vector of a point-pencil, i.e. all lines through the fixed point p. Moreover, $\mathcal{L}$ admits a parameter x for which hold that $|\mathcal{L}| = x\frac{q^n-1}{q-1}$. For CLLCs in $\mathrm{PG}(n,q)$, n odd, it has been proven that this definition is equivalent with the property that for every line spread $\mathcal{S}$ it holds that $|\mathcal{L} \cap \mathcal{S}| = x$. This result gives another perspective of these line sets and was obtained by using a known symmetric 3-class association scheme on the lines, i.e. the Grassmann association scheme.

Similarly, the same strategy can be used for CLLCs in $\mathrm{AG}(n,q)$, for general n. This technique constructs a symmetrical 4-class association scheme on the lines of $\mathrm{AG}(n,q)$ that results in a similar equivalent property. This talk will focus on the proof of this result and the construction of this 4-class association scheme. Furthemore, these results can be found in [1].

Keywords: Cameron-Liebler line classes, Association schemes, Affine space, Projective space

References

[1] J. D'haeseleer, J. Mannaert, F. Ihringer, and L. Storme. Cameron-Liebler k-sets in $\mathrm{AG}(n,q)$. *Elec. J. Combin.*, 28(4):11, 2021.

Rumi Melih Pelen, Erzurum Technical University

On the relationship between irreducible cyclic codes, finite projective planes and non-weakly regular bent functions

It is known that there is a one-to-one correspondence between irreducible cyclic codes over finite fields and multiplicative subgroups of finite fields. Namely, q being a prime power, and choosing a multiplicative subgroup of order n of a finite fields of order q^m as a defining set, one can obtain an irreducible cyclic $[n, m_0]$ code over $\mathbb{F}_q$ based on the generic construction method introduced by C. Ding, where m_0 divides m. The main problem is to evaluate the weight distribution of these codes, which depends on the Gaussian periods of the cyclotomic classes of order N in $\mathbb{F}_{q^m}$, where $q^m - 1 = nN$. In our paper "Strongly regular graphs arising from non-weakly regular bent functions" we observed that two disjoint subsets, $B_+(f)$ and $B_-(f)$, of the finite fields of order 3^6 obtained by partitioning the field with respect to the signs of the Walsh spectrum of a sporadic example of ternary non-weakly regular bent function f could be written as a union of certain cosets of the cyclotomic classes of order 13 in $\mathbb{F}_{3^6}$. Furthermore, we observe that irreducible cyclic code obtained by using the multiplicative subgroup of order 56 in $\mathbb{F}_{3^6}$ as a defining set is three-weight. As a union of certain cosets of this defining set in $\mathbb{F}_{3^6}, B_+(f)$ and $B_-(f)$ give rise to fusion schemes of class 2 (strongly regular graphs), and so two-weight projective linear codes. In this talk, after reviewing the general features, I will survey our further observations on the relationship between those structures and finite projective planes.

Session 4: 16:00 – 17:15

Shikha Patel, Indian Institute of Technology Patna

(θ, δ_θ)-cyclic codes over $\mathbb{F}_q[u,v]/\langle u^2-u, v^2-v, uv-vu\rangle$

Let $\mathbb{F}_q$ be the finite field of order $q = p^m$, where p is a prime, m is a positive integer, and $R = \mathbb{F}_q[u,v]/\langle u^2 - u, v^2 - v, uv - vu\rangle$. The ring $R[x;\theta,\delta_\theta]$ is noncommutative, known as skew polynomial ring, where θ is an

automorphism of R and δ_θ is a θ-derivation of R. The main concern of this work is to characterize (θ, δ_θ)-cyclic codes over R. Towards this, first we establish existence of the right division algorithm in $R[x; \theta, \delta_\theta]$. Then we find generating polynomials and idempotent generators for (θ, δ_θ)-cyclic codes over R. Moreover, it is shown that (θ, δ_θ)-cyclic codes are principally generated. Finally, by using the decomposition method, we have provided several examples of (θ, δ_θ)-cyclic codes of different lengths over R out of them many are optimal as per the available database.

José Manuel Muñoz, Universidad de Granada

A Generalized Euclidean Algorithm for Multisequence Skew-Feedback Shift-Register Synthesis

The problem of synthesizing a skew-feedback shift register of minimum length that generates a given set of sequences appears as a step towards decoding skew cyclic codes beyond their BCH bound by using multiple syndrome sequences. This problem was solved by Sidorenko et al. By extending the work from Feng and Tzeng into a skew-polynomial setting, an alternative solution is obtained, which relies on a generalized Euclidean algorithm working under a generalized skew polynomial division algorithm. This can be applied in order to develop a Sugiyama-like decoding algorithm for skew cyclic codes up to their Hartmann-Tzeng bound or their Roos bound.

References

[1] G. N. Alfarano, F. J. Lobillo and A. Neri. Roos bound for skew cyclic codes in Hamming and rank metric. *Finite Fields and Their Applications*, 69: 101772, 2021.

[2] G. L. Feng and K. K. Tzeng. A Generalized Euclidean Algorithm for Multisequence Shift-Register Synthesis. *IEEE Transactions on Information Theory*, 35(3): 584–594, 1989.

[3] J. Gómez-Torrecillas, F. J. Lobillo and G. Navarro. A Sugiyama-Like Decoding Algorithm for Convolutional Codes *IEEE Transactions on Information Theory*, 63(10): 6216–6226, 2017.

[4] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro ans A. Neri. Hartmann-Tzeng bound and skew cyclic codes of designed Hamming distance. *Finite Fields and Their Applications*, 50: 84–112, 2018.

[5] V. Sidorenko, L. Jiang and M. Bossert. Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes. *IEEE Transactions on Information Theory*, 57(2): 621–632, 2011.

Shikha Yadav, Indian Institute of Technology Patna

Self-dual and LCD double cirbulant codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$

Let q be an odd prime power, and denote by $\mathbb{F}_q$ the finite fields with q elements. In this paper, we consider the ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu = 0$ and study double circulant codes over this ring. We first obtain the necessary and sufficient conditions for a double circulant code to be self-dual (resp. LCD). Then we enumerate self-dual and LCD double circulant codes over R. Last but not the least, we show that the family of Gray images of self-dual and LCD double circulant codes over R are good.

Keywords: Double circulant code, Self-dual code, LCD code, Gray map.
